WHAT IS CLAIMED IS:

1. A method for supporting an establishment of a communication channel between a client computer capable of accessing an information storage medium which stores predetermined information contents and a connection information including medium identification data and a first remote server providing services related to the information contents through a open communication network, wherein said method comprises the steps of:

(a) providing a second remote server comprising means for storing medium identification reference data required to be identical with the medium identification data;

(b) receiving a connection authentification request message including the medium identification data from the client computer through the open communication network; and

(c) when the medium identification data is same as the medium identification reference data, generating an access code and transmitting an encrypted access code to the client computer, so that the client computer tries to establish a connection to the first remote server using the access code and receive the services.

2. The method as claimed in claim 1, wherein said step (c) comprises the steps of:

(c1) generating the access code;

(c2) encrypting the access code; and

(c3) transmitting an encrypted access code to the client computer through the open communication network.

3. The method as claimed in claim 2, further comprising the step of:

(d) transmitting an authentification notifying message including the access code to the first remote server, so that the first remote server provides the services to the client computer after verifying validity of the access code when the client computer requests a connection.

21

4.   The method as claimed in claim 3, wherein, in said step (b), the connection authentification request message further includes an address of the client computer on the open communication network,

wherein, in said step (d), the authentification notifying message further includes the address of the client computer,

wherein the first remote server verifies validity of the access code as well as the validity of the address of the client computer when the client computer requests the connection.

5.   The method as claimed in claim 3, wherein the authentification notifying message further includes time data for setting an expiration period of the access code, so that the first remote server invalidates the access code when the client computer does not request the connection within the expiration period.

6.   The method as claimed in claim 2, wherein at least a portion of the connection authentification request message is encrypted according to a predetermined encryption algorithm,

wherein said step (b) comprises a step of: decrypting the encrypted portion of the connection authentification request message.

7.   The method as claimed in claim 6, wherein, in said step (b), the connection authentification request message further includes an address of the client computer on the open communication network,

wherein, in said step (d), the authentification notifying message further includes the address of the client computer,

wherein the first remote server verifies validity of the access code as well as the address of the client computer when the client computer requests the connection.

8.   The method as claimed in claim 1, wherein both the first and the second remote servers are implemented in a same physical server and assigned with the same network address with each other.

22

9.   The method as claimed in claim 8, wherein the access code includes a Cookie value transmitted from the second remote server to the client computer through a Cookie-setting field to be stored in the client computer.

10.   A computer readable medium storing a program for setting up a communication channel between a client computer and a first remote server through an open communication network in a condition that the client computer can access an information storage medium storing predetermined information contents and a connection information including medium identification data and address data of a second remote server, said program carries out the functions of:

(a) making a connection authentification request message generated based on the connection information to be transmitted to the second remote server through the open communication network;

(b) receiving and decoding a connection authentification message provided by the second remote server in response to the connection authentification request message to recover an access code assigned by the second remote server; and

(c) providing the access code to a predetermined client program operating in the client computer so that the client program tries to establish a connection to the first remote server using the access code and receive services related to the information contents from the first remote server.

11.   The computer readable medium as claimed in claim 10, wherein the computer readable medium is the same as the information storage medium, and thus the information contents, the connection information, and the program are stored in a single medium.

12.   The computer readable medium as claimed in claim 10, wherein said function (a) comprises the functions of:

(a1) reading out the medium identification data and the address data of the second remote server from the information storage medium; and

23

5   (a2) providing the client program with the medium identification data and
6   the address data of the second remote server, so that the client program generates the
7   connection authentification request message using the medium identification data and
8   transmits the connection authentification request message to the second remote server.

1   13.   The computer readable medium as claimed in claim 12, wherein said
2   function (a2) comprises the functions of:
3   (a2a) encrypting the medium identification data; and
4   (a2b) providing the client program with an encrypted medium
5   identification data and the address data of the second remote server.

1   14.   The computer readable medium as claimed in claim 10, wherein said
2   function (a) comprises the functions of:
3   (a1) reading out the medium identification data and the address data of
4   the second remote server from the information storage medium; and
5   (a2) generating the connection authentification request message using
6   the medium identification data; and
7   (a3) making the connection authentification request message to be
8   transmitted to the second remote server.

1   15.   The computer readable medium as claimed in claim 14, wherein said
2   function (a2) comprises the function of: encrypting at least a portion, including the
3   medium identification data, of the connection authentification request message.

1   16.   The computer readable medium as claimed in claim 14, wherein said
2   function (a3) comprises the function of: transferring the connection authentification
3   request message to the client program, so that the client program transmits the
4   connection authentification request message to the second remote server.

1   17.   The computer readable medium as claimed in claim 14, wherein said
2   function (a3) comprises the function of: directly transmitting, without an intervention of

24

3   the client program, the connection authentification request message to the second

4   remote server.

1   18.   The computer readable medium as claimed in claim 10, wherein, in said

2   function (a), the connection authentification request message further includes an

3   address of the client computer on the open communication network.